REMARKS

Claims 1-38 are pending in the present application. No claims were canceled or added. Claim 23 was amended. In claim 23, the word "method" was changed to "data processing system." Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 103, Obviousness, Claims 1, 5, 7, 13, 15, 19, 21, 27, 31 and 33

The Examiner has rejected claims 1, 5, 7, 13, 15, 19, 21, 27, 31 and 33 under 35 U.S.C. § 103 as being unpatentable over Brickell, U.S. Patent No. 6,834,112 in view of Dietz et al, U.S. Patent No. 6,665,725B1. This rejection is respectfully traversed.

With regard to Claim 1, the Examiner stated:

> Regarding **claims 1 and 15**, Brickell teaches the invention substantially as claimed. Brickell discloses a method and means in a data processing system for processing a request, the method and means comprising:
>
> receiving the request (*column 3, lines 38-46*);
>
> responsive to a first hash value being present within the request, comparing the first hash value to a second has value, wherein the second hash value represents a current policy configuration (*column 2, lines 57-64; column 4, lines 24-48*) and
>
> a match between the first hash value and the second hash value.
>
> However, Brickell fails to teach, responsive to the match setting a quality of service based on information or policy configuration associated with the first hash value.
>
> In the same field of endeavor, Dietz discloses a (compiling statistics from a hash algorithm that provides analysis for measuring the quality of service based on many configurations…) [See Dietz, *column 17, lines 29-61*].
>
> Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Dietz's teachings of a method and apparatus to use hash value to set the quality of service, with the teachings of Brickell, for the purpose of "*allowing high packet rates to be successfully monitored in a network*" as stated by Dietz in lines 30-32 of column 13. Thus, Brickell also provides motivation to

> combine by stating a need to also provide to the network with "*the ability to more effectively distribute private keys in an insecure network to various terminals...*" [see Brickell, *column 2, lines 28-30*]. By this rationale **claims 1** and **15** are rejected.

Office Action dated February 9, 2005, pages 2-3.

A fundamental notion of patent law is the concept that invention lies in the new combination of old elements. Therefore, a rule that every invention could be rejected as obvious by merely locating each element of the invention in the prior art and combining the references to formulate an obviousness rejection is inconsistent with the very nature of "invention." Consequently, a rule exists that a combination of references made to establish a *prima facie* case of obviousness must be supported by some teaching, suggestion, or incentive contained in the prior art which would have led one of ordinary skill in the art to make the claimed invention.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

Additionally, in comparing Brickell to the claimed invention, the claim limitations of the presently claimed invention may not be ignored in an obviousness determination.

Independent claim 1, which is representative of independent claims 15 and 27 with regard to similarly recited subject matter, recites:

> 1. A method in a data processing system for processing a request, the method comprising:
>
> receiving the request;
>
> responsive to a first hash value being present within the request, comparing the first hash value to a second hash value, wherein the second hash value represents a current policy configuration for a quality of service; and
>
> responsive to a match between the first hash value and the second hash value, setting a quality of service based on information associated with the first hash value.

Brickell does not teach or suggest all the claim limitations in independent claim 1. Specifically, Brickell does not teach the feature of "responsive to a first hash value being present within the request, comparing the first hash value to a second hash value, wherein the second hash value represents a current policy configuration for a quality of service." Such a feature is not taught or suggested by Brickell. Therefore, claim 1 is not obvious in view of Brickell because the features believed to be disclosed by this cited reference are not present.

The Examiner points to column 2, lines 57 through 64 and column 4, lines 24 through 48 of Brickell as teaching the feature of "responsive to a first hash value being present within the request, comparing the first hash value to a second hash value, wherein the second hash value represents a current policy configuration for a quality of service." The two passages read as follows:

> As described herein, a user may sign or decrypt messages from multiple different client computers. For each different client computer, the user's private key is provided from a key server to the user in an encrypted format. A first hash of the user's password is used to authenticate the user and a second hash of the user's password is used to decrypt the user's private key. The user only has to remember one login name and a single associated password.

(Brickell, col. 2, lines 57 - 64)

> User 120 begins by inputting a login name **201** and a password **202**. (Act **301** in **FIG. 3**). Cryptographic programs **130** each contain two random numbers **205** and **206**, called Salt1 and Salt2, respectively. Salt1 **205** and Salt2 **206** are identical across the cryptographic programs **130** stored at each of client computers **108**. Salt1 **205**, password **202**, and optionally, login name **201** are input to a first hashing algorithm **203**. Similarly, Salt2 **206**, password **202**, and optionally, login name **201** are input to a second hashing algorithm **204**. Based on these inputs, first and second hashing algorithms **203** and **204** generate first and second hash codes (labeled "Hash1" and "Hash2," respectively). (Act **302**).
>
> The first and second hashing functions **203** and **204** may implement different mathematical hashing functions or the same hashing function. One suitable hashing algorithm for the first and second hashing functions **203** and **204** is the 160 bit SHA hashing

> algorithm. For any input string, SHA generates a 160 bit output valuc. The SHA hashing algorithm is well known in the cryptographic art. The hashing functions **203** and **204** may repeat the hashing algorithm multiple timcs in order to increase the difficulty of a brute force attack on the passwords. One suitable method for repeating SHA multiple times is with the PKCS # 5 algorithm, available from RSA, Inc., of Bedford, Mass.

(Brickell, col. 4, lines 24 – 48)

The first passage cited above, Brickell, column 2, lines 57 through 64, does not teach the feature of "responsive to a first hash value being present within the request, comparing the first hash value to a sccond hash valuc, wherein the second hash value represents a current policy configuration for a quality of service." Instead, the above cited passage teaches making two hashes of the user's password. Thc above cited passage does not teach "wherein the second hash value represents a current policy configuration for a quality of service." Instead, the above cited teachcs that the second hash is a hash of the user's password.

The second passagc cited above, Brickell, column 4, lines 24 through 48, does not teach the feature of "responsive to a first hash value being present within the request, comparing the first hash valuc to a second hash value, wherein the second hash value represents a current policy configuration for a quality of service." Instead, the abovc cited second passage of Brickell teaches that the user's password is combined with a random number, and possibly the user's login namc, to create a string that is hashed to form a first hash. Additionally, the above cited second passage of Brickcll teaches that the user's password is combined with a second random number, which is a different random number from the one used to generate the first hash, and possibly the user's login name, to create a string that is hashed to form a second hash. .

Furthermore, neither of the above cited passages is concerned with policies. The MPEP § 2173.05(a) states "When the specification states the meaning that a term in the claim is intended to have, the claim is examined using that meaning, in order to achieve a complete exploration of the applicant's invention and it's

PAGE 15/36 * RCVD AT 4/29/2005 11:15:50 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):11-04

relation to the prior art." *In re Zeltz,* 893 F.2d 319, 13 USPQ2d 1320 (Fed. Cir. 1989). The specification, on page 9, lines 26 through 28, defines the term "policy" as "a set of rules, also referred to as policy rules, used to handle packets." The two above cited passages teach creating hashes in order to verify the identity of user so that the user may have a private key distributed to the user, as explained in the abstract:

> A private key may be securely distributed to a user of a remote client computer over an insecure channel. The user's private key is transmitted to the client from a remote server in an encrypted format. A first hash of the user's password is transmitted to the remote server and is used to authenticate the user. A second hash of the user's password remains with the client computer and is used to decrypt the user's private key. The user only has to remember one login name and a single associated password. Thus, the private key can be securely distributed from the remote server to the client computer system.

The Brickell reference is not concerned with packets or policies for handling packets. Therefore, neither of the above cited passages of Brickell teaches the feature of "responsive to a first hash value being present within the request, comparing the first hash value to a second hash value, wherein the second hash value represents a current policy configuration for a quality of service." Thus, Brickell does not teach the feature of "responsive to a first hash value being present within the request, comparing the first hash value to a second hash value, wherein the second hash value represents a current policy configuration for a quality of service." Therefore, Brickell does not teach the claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

Furthermore, Dietz does not cure the deficiencies of Brickell. Dietz does not teach the feature missing from Brickell, "responsive to a first hash value being present within the request, comparing the first hash value to a second hash value, wherein the second hash value represents a current policy configuration for a quality of service," nor does the Examiner point to any portion of Dietz that teaches this feature.

Neither Brickell, Dietz nor the combination of Brickell and Dietz teaches the feature of "responsive to a match between the first hash value and the second hash value, setting a quality of service based on information associated with the first hash value." The Examiner points to Dietz, column 17, lines 29 through 61, reproduced below for the Examiner's convenience, as teaching this feature:

> Thus, in **804**, the system looks up the cache for a bucket from that bin using the hash. If the cache successfully returns with a bucket from the bin number, indicating there are more buckets in the bin, the lookup/update engine compares (**807**) the current signature (the UFKB-entry's signature) from that in the bucket (i.e., the flow-entry signature). If the signatures match (test **808**), that record (in the cache) is marked in step **810** as "in process" and a timestamp added. Step **811** indicates to the UFKB that the UFKB-entry in **802** has a status of "found." The "found" indication allows the state processing **328** to begin processing this UFKB element. The preferred hardware embodiment includes one or more state processors, and these can operate in parallel with the lookup/update engine.
>
> In the preferred embodiment, a set of statistical operations is performed by a calculator for every packet analyzed. The statistical operations may include one or more of counting the packets associated with the flow; determining statistics related to the size of packets of the flow; compiling statistics on differences between packets in each direction, for example using timestamps; and determining statistical relationships of timestamps of packets in the same direction. The statistical measures are kept in the flow-entries. Other statistical measures also may be compiled. These statistics may be used singly or in combination by a statistical processor component to analyze many different aspects of the flow. This may include determining network usage metrics from the statistical measures, for example to ascertain the network's ability to transfer information for this application. Such analysis provides for measuring the quality of service of a conversation, measuring how well an application is performing in the network, measuring network resources consumed by an application, and so forth.

However, the above cited passage does not teach the feature of "responsive to a match between the first hash value and the second hash value, setting a quality of service based on information associated with the first hash value." Instead, as stated by the Examiner, the above cited passage teaches "compiling statistics from a hash algorithm that provides analysis for measuring the quality of service based on many configurations." Officc Action dated February 9, 2005, pages 3 (emphasis added). Measuring the quality of service is different than setting the quality of service. Therefore, Dietz does not teach the feature of "responsive to a match between the first hash value and the second hash value, setting a quality of service based on information associated with the first hash value." Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

Additionally, stating that it is obvious to try or make a modification or combination without a suggestion in the prior art is not *prima facie* obviousness. The mere fact that a prior art reference can be readily modified does not make the modification obvious unless the prior art suggested the desirability of the modification. *In re Laskowski*, 871 F.2d 115, 10 U.S.P.Q.2d 1397 (Fed. Cir. 1989) and also *see In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992) and *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1993). The Examiner may not merely state that the modification would have been obvious to one of ordinary skill in the art without pointing out in the prior art a suggestion of the desirability of the proposed modification.

Obviousness under section 103 is directed to **compositions** and **methods**, and not making **efforts** and **attempts**. Slight reflection suggests that there is an element of "obvious to try" in any research endeavor, that it is not undertaken with complete blindness but rather with some semblance of a chance of success, and patentability determinations based on that as a test would result in a marked deterioration of the entire patent system as an incentive to invest in those efforts and attempts which go by the name research. Therefore, a modification or combination is obvious only if it is obvious to do from some teaching or suggestion in the prior art with a reasonable expectation of success.

The Examiner has failed to provide any motivation to combine the cited references. "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such

PAGE 18/36 * RCVD AT 4/29/2005 11:15:50 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):11-04

reference fairly suggests to one of ordinary skill in the art." *In re Hedges*, 228 U.S.P.Q. at 687. Thus, when Brickell is examined as a whole, Brickell teaches one of ordinary skill in the art a method for managing private keys in a public key cryptography system. Dietz is directed towards "allowing high packet rates to be successfully monitored in a network." (Dietz, col. 13, lines 30-32). Neither reference teaches anything about the problem or source of the other reference. Therefore, one of ordinary skill in the art would not be motivated to make the Examiner's proposed changes.

Furthermore, no motivation exists to combine the cited references. The present invention recognizes the need for an improved method of classifying packets in order to decrease the time needed to route a package to its destination. Brickell docs not teach the problem or its source. Instead, Brickell is directed towards managing private keys in a public key cryptography system. Neither does Dietz teach the problem or its source. Instead, Dietz is directed towards "allowing high packet rates to be successfully monitored in a network." (Dietz, col. 13, lines 30-32). Neither of the cited references teaches the problem or source of the problem solved by the present invention. Therefore, one of ordinary skill in the art would not be motivated to combine or modify the references in the manner required to form the solution disclosed in the claimed invention. Accordingly, it is not possible to state a *prima facie* case of obviousness.

Furthermore, even if Brickell and Dietz could be properly combined, a combination of Brickell and Dietz would not form the presently claimed invention in claim 1. Instead, a combination of Brickell and Dietz would, at best, result in a method for managing private keys in a public key cryptography system that uses two different hashes to verify security, which can also provided a stoical analysis of packet rates in a network. Therefore, the combination of Brickell and Dietz would not reach the presently claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

Therefore, for all the reasons set forth above, Applicants submit that independent claims 1, 15 and 27 are not taught or suggested by the alleged combination of Brickell and Dietz.

With regard to Claim 13, the Examiner stated:

> Regarding **claim 13**, the combination Brickell-Dietz teaches a data processing system comprising:
>
> a bus system [*see Dietz, fig. 10, items 1003-1004; column 18, lines 41-53*];
>
> a communications unit connected to the bus system [*see Dietz, fig. 10, items 1122; column 20, lines 6-21*];
>
> a memory connected to the bus system, wherein the memory includes a set of instructions [*see Dietz, fig. 10, items 1008, 1010; column 19, lines 36-61*]; and
>
> a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive the request [*see Dietz, fig. 11, items 1108; column 20, lines 15-31*]; compare the first hash value to a second hash value in response to a first hash value being present within the request, wherein the second hash value represents a current policy configuration for a quality of service [*see Dietz, column 17, lines 29-61*]; and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value in response to a match between the first hash value and the second hash value [*see Brickell, column 2, lines 57-64; column 4, lines 24-67; column 5, lines 1-8*]. The same motivation that was utilized in the combination of claim 1, applies equally as well to claim 13 [*see Dietz, column 13, lines 30-32*]. By this rationale **claim 13** is rejected.

Office Action dated February 9, 2005, pages 4-5.

Independent claim 13 recites:

> 13. A data processing system comprising:
>
> a bus system;
>
> a communications unit connected to the bus system;
>
> a memory connected to the bus system, wherein the memory includes a set of instructions; and
>
> a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive the request; compare the first hash value to a second hash value in response to a first hash value being present within the request, wherein the second hash value represents a current policy configuration for a quality of service; and set a quality of service based on information associated with the first hash value in

> response to a match between the first hash value and the second hash value.

Brickell does not teach or suggest all the claim limitations in independent claim 13. Specifically, Brickell does not teach the feature of "and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value." Such a feature is not taught or suggested by Brickell. Therefore, claim 13 is not obvious in view of Brickell because the features believed to be disclosed by this cited reference are not present.

On pages 2 and 3 of the Office Action dated February 9, 2005, when objecting to similar language contained in claim 1 of the present invention, the Examiner admits that "Brickell fails to teach, responsive to the match setting a quality of service based on information or policy configuration associated with the first hash value."

The Examiner points to two passages in Brickell, column 2, lines 57 through 64 and column 4, lines 24 through 67, cited above, as teaching the feature of "and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value." However, as was discussed above regarding independent claims 1 and 15, these two passages of Brickell do not teach this feature. Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

The Examiner also points to column 5, lines 1 through 8 of Brickell as teaching the feature of "and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value." Brickell, column 5, lines 1 through 8 states:

> Key server cryptographic program **150** authenticates the user by matching the transmitted login name and Hash1 to the corresponding values in table **250** (i.e., entries **251** and **252**). If the values match, the user is assumed to be the user specified by the login name, and the user's wrapped private key (entry **253**) is

> transmitted back to the user. (Acts **304**, **305**). If the values do not match, an error message is returned to the user. (Acts **304**, **306**).

The above cited passage of Brickell does not teach the feature of "and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value." Instead, the above cited passage teaches comparing the transmitted user name and hash1 to values stored in a table and returning the user's wrapped private key to the user. Sending a wrapped, or encoded private key to a user is different than "and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value."

Furthermore, Brickell does not teach "quality of service." Page 3, lines 23 through 24, states that "[t]he ability to define a level of performance is called a quality of service (QoS)." As was discussed above regarding independent claim 1, Brickell is concerned with being able to securely transfer a private key over an insecure network. Brickell has nothing to do with quality of service and does not teach quality of service or "and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value."

Thus, Brickell does not teach the feature of "and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value." Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

Furthermore, Dietz does not cure the deficiencies of Brickell. Dietz does not teach the feature missing from Brickell, "and set a quality of service based on information associated with the first hash value in response to a match between the first hash value and the second hash value," nor does the Examiner point to any portion of Dietz that teaches this feature.

Additionally, claim 13 recites the feature of "compare the first hash value to a second hash value in response to a first hash value being present within the request, wherein the second hash value represents a current policy configuration for a quality of service." Dietz does not teach or suggest this feature. The Examiner points to column 17, lines 29 through 61 of Dietz, cited above, as teaching this feature.

As was discussed above regarding independent claims 1 and 15, column 17, lines 29 through 61 of Dietz teaches performing a set of statistical analysis on every packet analyzed. The analysis covers a variety of characteristics including measuring some aspects of the quality of service. However, nowhere does this passage mention comparing values or the use of hash values. On page 14, lines 21 through 24 of the specification, a hash value is defined as "[a] hash algorithm is an algorithm that turns a variable-sized amount of text into a fixed-sized output, which is referred to as a hash value." Therefore, a statistical analysis or the result of a statistical analysis is not a hash value. Thus, Dietz does not teach the feature of "compare the first hash value to a second hash value in response to a first hash value being present within the request, wherein the second hash value represents a current policy configuration for a quality of service." Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

Therefore, for all the reasons set forth above, Applicants submit that independent claim 13 is not taught or suggested by the alleged combination of Brickell and Dietz.

Claims 5, 7, 19, 21, 31 and 33 are dependent claims depending from independent claims 1, 13, 15 and 27. As Applicants have already demonstrated that independent claims 1, 13, 15 and 27 are patentable over the Brickell and Dietz references, Applicants submit that dependent claims 5, 7, 19, 21, 31 and 33 are patentable over the Brickell and Dietz references at least by virtue of depending from an allowable claim.

Therefore, the rejection of claims 1, 5, 7, 13, 15, 19, 21, 27, 31 and 33 under 35 U.S.C. § 103 has been overcome.

PAGE 23/36 * RCVD AT 4/29/2005 11:15:50 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:9723857766 * DURATION (mm-ss):11-04

II. 35 U.S.C. § 103, Obviousness, Claims 6, 8-11, 22-25, 34-35 and 37

The Examiner has rejected claims 6, 8-11, 22-25, 34-35 and 37 under 35 U.S.C. § 103 as being unpatentable over Brickell in view of Farber et al, U.S. Patent No. 6,185,598B1. This rejection is respectfully traversed.

With regard to Claim 8, the Examiner stated:

> Regarding **claim 8**, the combination Brickell-Farber teaches a method in a data processing system for processing a request, the method comprising:
>
> responsive to receiving a request containing a selected cookie in which the selected cookie [*see Farber, column 23, lines 20-62*] includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system [*see Brickell, column 4, lines 24-67; column 5, lines 1-42*]; and
>
> responsive to a correspondence between the first hash value and the second hash value, processing the request using the information [*see Brickell, column 2, lines 57-64; column 4, lines 24-67*]. The same motivation that was utilized in the combination of claim 6, applies equally as well to claim 8 [*see Farber, column 23, lines 40-43*]. By this rationale **claim 8** is rejected.

Office Action dated February 9, 2005, pages 8-9.

A fundamental notion of patent law is the concept that invention lies in the new combination of old elements. Therefore, a rule that every invention could be rejected as obvious by merely locating each element of the invention in the prior art and combining the references to formulate an obviousness rejection is inconsistent with the very nature of "invention." Consequently, a rule exists that a combination of references made to establish a *prima facie* case of obviousness must be supported by some teaching, suggestion, or incentive contained in the prior art which would have led one of ordinary skill in the art to make the claimed invention.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

Additionally, in comparing Brickell to the claimed invention, the claim limitations of the presently claimed invention may not be ignored in an obviousness determination.

Independent claim 8, which is representative of independent claims 22 and 34 with regard to similarly recited subject matter, recites:

> 8. A method in a data processing system for processing a request, the method comprising:
> responsive to receiving a request containing a selected cookie in which the selected cookie includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system; and
> responsive to a correspondence between the first hash value and the second hash value, processing the request using the information.

Brickell does not teach or suggest all the claim limitations in independent claim 8. Specifically, Brickell does not teach the feature of "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system." Such a feature is not taught or suggested by Brickell. Therefore, claim 8 is not obvious in view of Brickell because the features believed to be disclosed by this cited reference are not present.

The Examiner points to column 4, line 24 through column 5, lines 42 of Brickell, reproduced below for the Examiner's convenience, as teaching the feature of "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system."

> User **120** begins by inputting a login name **201** and a password **202**. (Act **301** in FIG. **3**). Cryptographic programs **130** each contain two random numbers **205** and **206**, called Salt1 and Salt2, respectively. Salt1 **205** and Salt2 **206** are identical across the

cryptographic programs **130** stored at each of client computers **108**. Salt1 **205**, password **202**, and optionally, login name **201** are input to a first hashing algorithm **203**. Similarly, Salt2 **206**, password **202**, and optionally, login name **201** are input to a second hashing algorithm **204**. Based on these inputs, first and second hashing algorithms **203** and **204** generate first and second hash codes (labeled "Hash1" and "Hash2," respectively). (Act **302**).

The first and second hashing functions **203** and **204** may implement different mathematical hashing functions or the same hashing function. One suitable hashing algorithm for the first and second hashing functions **203** and **204** is the 160 bit SHA hashing algorithm. For any input string, SHA generates a 160 bit output value. The SHA hashing algorithm is well known in the cryptographic art. The hashing functions **203** and **204** may repeat the hashing algorithm multiple times in order to increase the difficulty of a brute force attack on the passwords. One suitable method for repeating SHA multiple times is with the PKCS # 5 algorithm, available from RSA, Inc., of Bedford, Mass.

In general, hashing algorithms take arbitrary strings as input, and produce an output of fixed size that is dependent on the input. Ideally, it should never be possible to derive the input data given the hash algorithm's output. For a hashing algorithm to be cryptographically secure, such as the SHA algorithm, it must be very difficult to find two input strings that produce the same output hash value, or to find an input string that produces a given hash value.

Because Salt1 and Salt2 are different values, hashing algorithms **203** and **204** will necessarily operate on different input strings and thus their output values, Hash1 and Hash2, will be, to a statistical certainty, different from one another.

Key server cryptographic program **150** includes a pre-stored table **250**. As shown in FIG. **2**, table **250** includes entries relating: the login names of the possible users of the key server (entry **251**), the first hash value (Hash1) associated with each of these login names (entry **252**), the wrapped user's private key (entry **253**), and the user's public key (entry **254**) (optional).

Key server cryptographic program **150** authenticates the user by matching the transmitted login name and Hash1 to the corresponding values in table **250** (i.e., entries **251** and **252**). If the values match, the user is assumed to be the user specified by the login name, and the user's wrapped private key (entry **253**) is

> transmitted back to the user. (Acts **304**, **305**). If the values do not match, an error message is returned to the user. (Acts **304**, **306**).
>
> The wrapped private key, when received by client cryptographic program **130**, is unwrapped using Hash2 as the key to symmetric decryption algorithm **208**. (Act **306**). Symmetric decryption algorithm **208** is the same algorithm used to initially wrap the private key, such as the DES algorithm. With the private key in hand, cryptographic program **130** may now use the private key for any cryptographic operation that requires the private key. If the private key is a digital signature key, the cryptographic program **130** could now sign messages with the private key. (Act **307**). If the private key is a decryption key, the cryptographic program **130** could now decrypt messages that were encrypted with the corresponding public encryption key (Act **307**). The private key may be used, for example, to sign messages sent to content server/relying party **102** or to encrypt messages sent to the content server/relying party **102**.
>
> The pre-generation of table **250** at key server **101** will now be described in more detail with reference to FIG. **4**. The user registers a private key/public key pair with key server **101** by first entering a login name and password. (Act **401**). Hash**1** and Hash**2** are then generated as described above in Act **302**. (Act **402**). If the user does not have a public key/private key pair, cryptographic program **130** generates these keys for the user, (Act **403**), and encrypts the user's private key with a symmetric encryption algorithm, using Hash2 or a value derived from Hash2 as the key for the symmetric encryption algorithm. (Act **404**). As discussed above, encrypting a private key using a symmetric encryption algorithm is commonly referred to as "wrapping" the private key. The symmetric encryption algorithm may be, for example, the well known Triple DES algorithm. The key used to wrap the user's private key is preferably at least 100 bits in length.

The above cited passage of Brickell does not teach the feature of "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system." Instead, the above cited passage of Brickell teaches that the user's password is combined with a random number, and possibly the user's login name, to create a string that is hashed to form a first hash, Hash1. Additionally, the above cited passage of Brickell teaches that the user's password is combined with a second random number, which is a different random number from the one used to generate the first hash, and possibly the user's login name, to create a string that is hashed to form a second hash, Hash2. The passage also teaches that Hash2 is used to wrap or encrypt the user's private key. The above cited passage does not teach the feature of "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system." Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

Furthermore, the above cited passage does not teach "policies" or "wherein the second hash value represents a current policy configuration for processing requests by the data processing system." The MPEP § 2173.05(a) states "When the specification states the meaning that a term in the claim is intended to have, the claim is examined using that meaning, in order to achieve a complete exploration of the applicant's invention and it's relation to the prior art." *In re Zeltz*, 893 F.2d 319, 13 USPQ2d 1320 (Fed. Cir. 1989). The specification, on page 9, lines 26 through 28, defines the term "policy" as "a set of rules, also referred to as policy rules, used to handle packets." The above cited passage teaches creating hashes in order to verify the identity of user and to encrypt the user's private key so that the user may have a private key distributed to the user over an insecure connection, as explained in the abstract:

> A private key may be securely distributed to a user of a remote client computer over an insecure channel. The user's private key is transmitted to the client from a remote server in an encrypted format. A first hash of the user's password is transmitted to the remote server and is used to authenticate the user. A second hash of the user's password remains with the client computer and is used to decrypt the user's private key. The user only has to remember one login name and a single associated password. Thus, the private key can be securely distributed from the remote server to the client computer system.

The Brickell reference is not concerned with packets or policies for handling packets. Therefore, the above cited passage of Brickell does not teach "wherein the second hash value represents a current policy configuration for processing requests by the data processing system." Thus, Brickell does not teach the feature of "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system." Therefore, the proposed combination does not result in the claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

Furthermore, Farber does not cure the deficiencies of Brickell. Farber does not teach the feature missing from Brickell, "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system," nor does the Examiner point to any portion of Farber that teaches these features.

Additionally, stating that it is obvious to try or make a modification or combination without a suggestion in the prior art is not *prima facie* obviousness. The mere fact that a prior art reference can be readily modified does not make the modification obvious unless the prior art suggested the desirability of the modification. *In re Laskowski*, 871 F.2d 115, 10 U.S.P.Q.2d 1397 (Fed. Cir. 1989) and also *see In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992) and *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1993). The Examiner may not merely state that the modification would have been obvious to one of ordinary skill in the art without pointing out in the prior art a suggestion of the desirability of the proposed modification.

Obviousness under section 103 is directed to **compositions** and **methods**, and not making **efforts** and **attempts**. Slight reflection suggests that there is an element of "obvious to try" in any research endeavor, that it is not undertaken with complete blindness but rather with some semblance of a chance of success, and patentability determinations based on that as a test would result in a marked deterioration of the entire patent system as an incentive to invest in those efforts and attempts which go by the name research. Therefore, a modification or combination is obvious only if it is obvious to do from some teaching or suggestion in the prior art with a reasonable expectation of success.

The Examiner has failed to provide any motivation to combine the cited references. "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *In re Hedges*, 228 U.S.P.Q. at 687. Thus, when Brickell is examined as a whole, Brickell teaches one of ordinary skill in the art a method for managing private keys in a public key cryptography system. Farber is directed towards "a way for servers in a computer network to off-load their processing of requests for selected resources by determining a different server (a "repeater") to process those requests" (Farber, col. 2, lines 55-58). Neither reference teaches anything about the problem or source of the other reference. Therefore, one of ordinary skill in the art would not be motivated to make the Examiner's proposed changes.

Furthermore, no motivation exists to combine the cited references. The present invention recognizes the need for an improved method of classifying packets in order to decrease the time needed to route a package to its destination. Brickell does not teach the problem or its source. Instead, Brickell is directed towards managing private keys in a public key cryptography system. Neither does Farber teach the problem or its source. Instead, Farber is directed towards "a way for servers in a computer network to off-load their processing of requests for selected resources by determining a different server (a "repeater") to process those requests" (Farber, col. 2, lines 55-58). Neither of the cited references teaches the problem or source of the problem solved by the present invention. Therefore, one of ordinary skill in the art would not be motivated to combine or modify the references in the manner required to form the solution disclosed in the claimed invention. Accordingly, it is not possible to state a *prima facie* case of obviousness.

Furthermore, even if Brickell and Farber could be properly combined, a combination of Brickell and Farber would not form the presently claimed invention in claim 8. Instead, a combination of Brickell and Farber would result in method for managing private keys in a public key cryptography system that uses two different hashes to verify security, in which the request for access to the private key could be attached to a cookie. Therefore, the combination of Brickell and Farber would not reach the presently claimed invention. Accordingly, the Examiner has failed to state a case of *prima facie* obviousness.

Therefore, for all the reasons set forth above, Applicants submit that independent claims 8, 22 and 34 are not taught or suggested by the alleged combination of Brickell and Farber.

Claims 9-11, 23-25, 35 and 37 are dependent claims depending from independent claims 8, 22 and 34. As Applicants have already demonstrated that independent claims 8, 22 and 34 are patentable over the Brickell and Farber references, Applicants submit that dependent claims 9-11, 23-25, 35 and 37 are patentable over the Brickell and Farber references at least by virtue of depending from an allowable claim.

Furthermore, claim 6 is a dependent claim, depending from dependent claim 5, which depends from independent claim 1. In the rejection of claim 1, the Examiner cited the combination of Brickell and Dietz as teaching the features of claim 1. However, in the rejection of claim 6, the Examiner recasts the rejection of claim 1 and states that claim 5, which is dependent on claim 1, is taught by Brickell only, yet the Examiner provides no specific reference as to how Brickell does this. As such, Applicants are confused about how exactly to respond to this rejection. However, as Applicants have previously shown claim 1 to be in condition for allowance over the alleged combination of Brickell and Dietz, Applicants submit that claim 6 is also allowable at least by virtue of depending from an allowable claim.

Therefore, the rejection of claims 6, 8-11, 22-25, 34-35 and 37 under 35 U.S.C. § 103 has been overcome.

III. <u>35 U.S.C. § 103, Obviousness, Claims 2-4, 12, 14, 16-18, 20, 26, 28-30, 32, 36 and 38</u>

The Examiner has rejected claims 2-4, 12, 14, 16-18, 20, 26, 28-30, 32, 36 and 38 under 35 U.S.C. § 103 as being unpatentable over Brickell and Dietz as applied to claims 1, 15, and 27, and in further view of Farber. This rejection is respectfully traversed.

In the Office Action, the Examiner stated:

> Regarding **claim 14**, the combination Brickell-Dietz-Farber teaches a data processing system comprising:
>
> a bus system [*see Dietz, fig. 10, items 1003-1004; column 18, lines 41-53*];
>
> a communications unit connected to the bus system [*see Dietz, fig. 10, items 1122; column 20, lines 6-21*];
>
> a memory connected to the bus system, wherein the memory includes a set of instructions [*see Dietz, fig. 10, items 1008, 1010; column 19, lines 36-61*]; and
>
> a processing unit connected to the busy system, wherein the processing unit executes the set of instructions to determine whether the first hash value corresponds to a second hash value in response to receiving a request containing a selected cookie in which the selected cookie [*see Farber, column 23, lines 22-65*] includes a first hash value and information associated with the hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system; and process the request using the information in response to a correspondence between the first hash value and the second hash value [*see Brickell, column 2, lines 57-64, column 4, lines 24-67, column 5, lines 1-8*]. The same motivation that was utilized in the combination of claim 2, applies equally as well to claim 14 [*see Farber, column 23, lines 40-43*]. By this rationale **claim 14** is rejected.

Office Action dated February 9, 2005, page 15.

A fundamental notion of patent law is the concept that invention lies in the new combination of old elements. Therefore, a rule that every invention could be rejected as obvious by merely locating each element of the invention in the prior art and combining the references to formulate an obviousness rejection is inconsistent with the very nature of "invention." Consequently, a rule exists that a combination of references made to establish a *prima facie* case of obviousness must be supported by some teaching, suggestion, or incentive contained in the prior art which would have led one of ordinary skill in the art to make the claimed invention.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

Additionally, in comparing Brickell to the claimed invention, the claim limitations of the presently claimed invention may not be ignored in an obviousness determination.

Independent claim 14 recites:

> 14. A data processing system comprising:
> a bus system;
> a communications unit connected to the bus system;
> a memory connected to the bus system, wherein the memory includes a set of instructions; and
> a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to determine whether the first hash value corresponds to a second hash value in response to receiving a request containing a selected cookie in which the selected cookie includes a first hash value and information associated with the hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system; and process the request using the information in response to a correspondence between the first hash value and the second hash value.

Brickell does not teach or suggest all the claim limitations in independent claim 14. Specifically, Brickell does not teach the feature of "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system; and process the request using the information in response to a

DcLima et al. – 09/904,025

correspondence between the first hash value and the second hash value." Such a feature is not taught or suggested by Brickell. Therefore, claim 14 is not obvious in view of Brickell because the features believed to be disclosed by this cited reference are not present.

The Examiner points to column 2, lines 57 through 64 and column 4, line 24 through column 5, lines 8 of Brickell, cited above in regards to independent claims 1 and 8, as teaching the feature of "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system; and process the request using the information in response to a correspondence between the first hash value and the second hash value." As was discussed above regarding claim 8, Brickell does not teach this feature, nor does Farber cure Brickell's deficiencies. Dietz also does not cure the deficiencies of Brickell. As was discussed above regarding claim 1, Dietz teaches monitoring packet flows and doing statistical analysis of the packet flows. Dietz does not teach "includes a first hash value and information associated with the hash value, determining whether the first hash value corresponds to a second hash value, wherein the second hash value represents a current policy configuration for processing requests by the data processing system; and process the request using the information in response to a correspondence between the first hash value and the second hash value," nor does the Examiner point to portion of Dietz as teaching this feature.

Therefore, for all the reasons set forth above, Applicants submit that independent claim 14 is not taught or suggested by the alleged combination of Brickell and Dietz in view of Farber.

Claims 2-4, 16-18, 20, 28-30 and 32 are dependent claims which depend from independent claims 1, 15 and 27. As Applicants have already demonstrated that independent claims 1, 15 and 27 are patentable over the Brickell and Dietz references, Applicants submit that dependent claims 9-11, 23-25, 35 and 37 are patentable over the alleged combination of Brickell and Dietz further in view of Farber at least by virtue of depending from an allowable claim.

Claims 12, 26, 36 and 38 are dependent claims that depend from independent claims 8, 22 and 34. However, the Examiner has based his rejection on the alleged combination of Brickell and Dietz as applied to claims 1, 15 and 27 and then further in view of Farber. With regards to claim 12, the Examiner states that the alleged Brickell, Dietz and Farber combination teaches claim 8, yet in the rejection to claim 8 the Examiner only cites Brickell and Farber as allegedly teaching the features of claims 8. Similarly with regards to claims 22, 36 and 38, the Examiner states that that the alleged Brickell, Dietz and Farber combination teaches the underlying independent claim, yet in the rejection to those independent claims Examiner only cites Brickell and Farber as allegedly teaching the features of the claims. Furthermore, the Examiner does not cite Dietz in the rejection of any of the features of claims 12, 26, 36 and 38. Therefore Applicants are confused as to exactly how to properly respond to the rejections of claims 12, 26, 36 and 38. However, As Applicants have already demonstrated that independent claims 8, 22 and 34 are patentable over the Brickell and Farber references; Applicants submit that dependent claims 12, 26, 36 and 38. are patentable over the alleged combination of Brickell and Dietz further in view of Farber at least by virtue of depending from an allowable claim.

Therefore, the rejection of claims 2-4, 12, 14, 16-18, 20, 26, 28-30, 32, 36 and 38 under 35 U.S.C. § 103 has been overcome.

IV. Conclusion

It is respectfully urged that the subject application is patentable over Brickell and Dietz, Brickell and Farber, and Brickell, Dietz and Farber, and is now in condition for allowance.

The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: April 29, 2005

Respectfully submitted,

Gerald H. Glanzman
Reg. No. 25,035
Duke W. Yee
Reg. No. 34,285
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicant